					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P36S					Tytuł dokumentu: **Polityka mediów społecznościowych i komunikacji zewnętrznej**							
Wersja: 1.0		Data wejścia w życie: 01.01.2025			Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne	

Historia zmian				
Numer zmiany	**Data zmiany**	**Zmiany**	**Przegląd wykonał**	**Właściciel procesu**

Zatwierdzenia			
Imię i nazwisko	**Stanowisko**	**Data**	**Podpis**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzule 5.1, 5.2, 6.1, 8	Nadzór kierownictwa, zarządzanie ryzykiem oraz kontrola operacyjna komunikacji zewnętrznej
ISO/IEC 27002:2022	Środki kontrolne 5.10, 5.11	Dopuszczalne użytkowanie aktywów organizacji oraz bezpieczeństwo informacji w komunikacji
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	Zasady postępowania, audyt, zgłaszanie incydentów oraz zarządzanie treściami publicznie dostępnymi i dostępem
RODO	Artykuły 5, 32, 33	Zasady ochrony danych, bezpieczeństwo oraz zgłaszanie naruszeń mających wpływ na komunikację publiczną
Dyrektywa NIS2	Artykuł 21(2)(e), 21(2)(f)	Polityki dotyczące korzystania z systemów oraz zarządzania ryzykiem w łańcuchu dostaw i komunikacji publicznej
Rozporządzenie DORA	Artykuł 14(4)	Obowiązki komunikacyjne po incydentach

1. Cel

1.1. Niniejsza polityka ustanawia obowiązkowe zasady dla wszelkiej komunikacji publicznej, w tym korzystania z mediów społecznościowych, kontaktów z prasą oraz publikacji zewnętrznych treści cyfrowych, w przypadku odniesień do spółki, jej personelu, klientów, systemów lub praktyk wewnętrznych.

1.2. Celem polityki jest ochrona reputacji spółki, utrzymanie zgodności z wymaganiami prawnymi i regulacyjnymi oraz ograniczenie ryzyka wycieku informacji, dezinformacji lub incydentów bezpieczeństwa.

1.3. Polityka umożliwia personelowi i partnerom prowadzenie pozytywnej i odpowiedzialnej aktywności w dyskusjach online, przy jednoczesnym unikaniu przypadkowych ujawnień lub błędnego przedstawiania faktów.

1.4. Polityka wzmacnia gotowość SME do certyfikacji ISO/IEC 27001 poprzez uwzględnienie mechanizmów kontroli dotyczących informacji udostępnianych publicznie lub interesariuszom zewnętrznym.

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do wszystkich osób związanych z organizacją, w tym:

2.1.1. pracowników i kontrahentów

2.1.2. osób świadczących pracę na podstawie umów cywilnoprawnych, konsultantów i dostawców zewnętrznych

2.1.3. stażystów oraz personelu zatrudnionego w niepełnym wymiarze czasu pracy, zaangażowanych w realizację usług dla klientów lub mających dostęp do systemów

2.2. Polityka ma zastosowanie do wszystkich form komunikacji zewnętrznej odnoszącej się do organizacji, w tym:

2.2.1. wpisów w mediach społecznościowych (LinkedIn, Twitter/X, TikTok, Instagram, Facebook itp.)

2.2.2. wpisów blogowych, postów na forach internetowych, opinii klientów i wątków dyskusyjnych

2.2.3. wystąpień publicznych (np. konferencji, webinarów, podcastów)

2.2.4. wiadomości e-mail lub wiadomości kierowanych do dziennikarzy, przedstawicieli administracji publicznej lub influencerów

2.2.5. publicznie udostępnianych zrzutów ekranu, zdjęć lub nagrań wideo z miejsc pracy

2.3. Polityka ma również zastosowanie, gdy taka komunikacja jest prowadzona:

2.3.1. z prywatnych urządzeń lub kont

2.3.2. poza standardowymi godzinami pracy

2.3.3. bez zamiaru wyrządzenia szkody — nawet przypadkowe lub mimochodem wypowiedziane uwagi wchodzą w zakres niniejszej polityki, jeżeli odnoszą się do spółki

3. Cele

3.1. Ochrona reputacji: zapobieganie szkodom wizerunkowym spółki wynikającym z nieuprawnionej lub niewłaściwej komunikacji publicznej

3.2. Bezpieczeństwo danych: unikanie niezamierzonego ujawnienia danych wrażliwych, informacji o systemach wewnętrznych lub danych klientów za pośrednictwem mediów społecznościowych lub kanałów publicznych

3.3. Zgodność z wymaganiami prawnymi i regulacyjnymi: zapewnienie, że wszelkie treści publiczne odnoszące się do spółki są zgodne z obowiązującymi przepisami dotyczącymi ochrony danych i komunikacji biznesowej

3.4. Profesjonalne postępowanie: promowanie odpowiedzialnego udziału w dyskusjach online i kontaktach z mediami, również z kont prywatnych

3.5. Gotowość na incydenty: określenie jasnych i praktycznych działań na wypadek przypadkowych ujawnień lub naruszeń niniejszej polityki

4. Role i odpowiedzialności

4.1. Dyrektor Generalny (GM)

4.1.1. jest właścicielem niniejszej polityki i zatwierdza ją

4.1.2. dokonuje przeglądu i autoryzuje wszelkie oświadczenia publiczne, kontakty z prasą oraz wywiady dla mediów

4.1.3. zapewnia skuteczne zakomunikowanie niniejszej polityki wszystkim pracownikom i stronom trzecim

4.1.4. prowadzi postępowania wyjaśniające i podejmuje działania w odpowiedzi na wszelkie naruszenia niniejszej polityki, zgodnie z procedurami reagowania na incydenty

4.2. Wyznaczony pracownik lub osoba odpowiedzialna za komunikację (jeżeli została wyznaczona)

4.2.1. wspiera GM poprzez przegląd treści przed ich publikacją zewnętrzną (np. wpisów blogowych, tematów wystąpień)

4.2.2. prowadzi rejestry zatwierdzonej aktywności medialnej lub wpisów w mediach społecznościowych o podwyższonym ryzyku

4.2.3. monitoruje, w miarę dostępnych możliwości, znane wzmianki o spółce w Internecie pod kątem ryzyk reputacyjnych lub bezpieczeństwa

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Wymagania dotyczące przeglądu i aktualizacji

9.1. Coroczny przegląd

9.1.1. Niniejsza polityka musi być poddawana przeglądowi co najmniej raz w roku przez Dyrektora Generalnego (GM)

9.1.2. Przegląd musi zapewniać zgodność ze zaktualizowanymi obowiązkami prawnymi, trendami w komunikacji branżowej oraz wewnętrznymi zmianami biznesowymi

9.2. Przeglądy inicjowane zdarzeniem

9.2.1. Niniejsza polityka musi zostać zaktualizowana niezwłocznie po:

9.2.1.1. istotnym incydencie w mediach społecznościowych lub problemie reputacyjnym

9.2.1.2. zmianie zewnętrznych dostawców zarządzających komunikacją

9.2.1.3. wejściu w życie nowych przepisów lub obowiązków regulacyjnych dotyczących komunikacji online, mediów lub marki

9.3. Dokumentowanie zmian

9.3.1. Wszystkie aktualizacje muszą być rejestrowane, w tym data przeglądu, podsumowanie zmian oraz zatwierdzenie przez GM

9.3.2. Na potrzeby audytu i certyfikacji należy prowadzić historię wersji

9.4. Dystrybucja aktualizacji

9.4.1. Cały personel i kontrahenci muszą zostać poinformowani o wszelkich zmianach polityki

9.4.2. Zaktualizowane wersje muszą być udostępniane pocztą elektroniczną lub za pośrednictwem portali wewnętrznych

9.4.3. Każdy dostawca obsługujący komunikację publiczną musi potwierdzić przyjęcie zaktualizowanych warunków przed kontynuowaniem współpracy

10. Powiązane polityki i zależności

10.1. Niniejsza polityka funkcjonuje w powiązaniu z następującymi politykami SME:

10.1.1. P3S – Polityka dopuszczalnego użytkowania: określa dopuszczalne zachowania przy korzystaniu z platform komunikacyjnych, w tym dostępu do mediów społecznościowych w godzinach pracy

10.1.2. P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: zapewnia, że personel jest szkolony w zakresie identyfikacji ryzyka nadmiernego udostępniania informacji, phishingu lub zagrożeń reputacyjnych online

10.1.3. P17S – Polityka ochrony danych i prywatności: zapewnia, że dane osobowe i dane klientów nie są udostępniane w komunikacji zewnętrznej, zgodnie z RODO i innymi wymaganiami prawnymi

10.1.4. P30S – Polityka reagowania na incydenty: reguluje reakcję na przypadkowe ujawnienie publiczne, zagrożenia online lub ataki reputacyjne wynikające z niewłaściwego korzystania z mediów społecznościowych

10.1.5. P37S – Polityka zgodności prawnej i regulacyjnej: określa szersze obowiązki prawne i umowne organizacji przy publicznym udostępnianiu treści

10.2. Polityki te muszą być stosowane łącznie w celu utrzymania bezpiecznej, profesjonalnej i zgodnej z prawem obecności zewnętrznej.

11. Normy i ramy odniesienia

11.1. ISO/IEC 27001

11.1.1. Klauzula 5.1 – Przywództwo i zaangażowanie: wymaga nadzoru kierownictwa nad ryzykiem reputacyjnym i ryzykiem informacyjnym

11.1.2. Klauzula 6.1 – Zarządzanie ryzykiem bezpieczeństwa informacji: obejmuje ekspozycję na ryzyko związaną z komunikacją

11.1.3. Klauzula 8.1 – Kontrola operacyjna: obejmuje zasady dotyczące sposobu komunikowania informacji na zewnątrz

11.2. ISO/IEC 27002

11.2.1. Środek kontrolny 5.10 – Dopuszczalne użytkowanie informacji i aktywów

11.2.2. Środek kontrolny 5.11 – Bezpieczeństwo informacji w komunikacji

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Zasady postępowania: reguluje właściwe postępowanie przy korzystaniu z zasobów informacyjnych

11.3.2. AU-7 – Ograniczanie audytu i generowanie raportów: wspiera monitorowanie publicznego korzystania z systemów

11.3.3. IR-6 – Zgłaszanie incydentów: wymusza reakcję na naruszenia reputacyjne i naruszenia związane z komunikacją

11.3.4. AC-22 – Treści publicznie dostępne: zapewnia kontrolę nad publikacjami zewnętrznymi i dostępem

11.4. RODO (2016/679)

11.4.1. Artykuł 5 – Zasady dotyczące przetwarzania danych osobowych (dokładność, integralność, rozliczalność)

11.4.2. Artykuł 32 – Bezpieczeństwo przetwarzania: wymaga stosowania środków ochrony w zakresie publicznego udostępniania informacji

11.4.3. Artykuł 33 – Zgłoszenie naruszenia: ma zastosowanie, jeżeli dane osobowe zostaną ujawnione poprzez komunikację zewnętrzną

11.5. Dyrektywa NIS2 (2022/2555)

11.5.1. Artykuł 21(2)(e) – Polityki dotyczące korzystania z systemów informatycznych, w tym platform komunikacyjnych

11.5.2. Artykuł 21(2)(f) – Polityki dotyczące obsługi ryzyk cyberbezpieczeństwa w łańcuchu dostaw i na platformach publicznych

11.6. Rozporządzenie DORA (2022/2554)

11.6.1. Artykuł 14(4) – Obowiązki komunikacyjne wobec klientów, stron trzecich i organów po incydentach operacyjnych

11.7. COBIT 2019

11.7.1. APO09 – Zarządzanie umowami o poziomie usług: obejmuje nadzór nad dostawcami i stronami trzecimi związanymi z komunikacją

11.7.2. DSS05 – Zarządzanie usługami bezpieczeństwa: obejmuje ochronę publicznie dostępnych aktywów cyfrowych

11.7.3. EDM03 – Zapewnienie optymalizacji ryzyka: podkreśla zarządzanie ryzykiem reputacyjnym i ryzykiem zgodności związanym z komunikacją